UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/752,248	12/27/2000	Jacek Piotr Wysoczynski	42390P9693	7471

7590 02/11/2004

Joseph A Twarowski
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard 7th Floor
Los Angeles, CA 90025

EXAMINER	
BRANCOLINI, JOHN R	
ART UNIT	**PAPER NUMBER**
2153	3

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/752,248	WYSOCZYNSKI, JACEK PIOTR	
	Examiner	Art Unit	
	John R Brancolini	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-26 are pending in the application.

Priority

No claim for priority has been made in the application.

Specification

The disclosure is objected to because of the following informalities: A "Brief Summary of the Invention" is missing. According to 37 CFR 1.77, a "Brief Summary of the Invention" should follow the "Background of the Invention".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-10, 11-16, 18-23, 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gold et al. (European Patent EP 0899662 A1), hereinafter referred to as Gold, in view of Davis, Jr. et al. (US Patent 6334149), hereinafter referred to as Davis.

In regards to claim 1, Gold discloses a method comprising:

- Establishing a file transfer session between an information transferring network device that has entered a debug mode and a server, a name of a last known set of backup data being stored on the network device, the last known good backup data being stored on the server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050], the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Requesting a transfer of the last backup data from the server to the network device (the user requests the transfer of the backup files, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

Davis discloses a method of monitoring and recording critical system data in a device for initial program loading over a network. In the described invention, Davis teaches that a backup copy of a image and configuration file pair can be stored on a server to allow a client to load or boot a system with a reset initialization routine that will assure functionality (col 5 lines 15-42).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Gold's method of data backup and restoration to include utilizing an image and configuration file as taught by Davis to allow a client to load or boot a system with a reset initialization routine that will assure functionality.

In regards to claim 2, Gold discloses detecting the network device in fatal mode and entering the debug mode on the network device upon detecting the network device

in fatal mode (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).

In regards to claim 3, Gold discloses receiving a command of a user and entering the debug mode on the network device upon receiving the command of the user (a user can choose to enter the debug mode to restore the backup data, paragraphs [0049] – [0053]).

In regards to claim 5, Gold discloses transfer of the last known backup data from the server to the network device (paragraph [0051]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 1, Davis teaches the use of an image and configuration file pair.

In regards to claim 6, Gold discloses automatically restoring the network device from debug mode to working mode after receiving the transfer of the last known backup data from the server to the network device (the transfer is starts, proceeds and finishes unattended which would show that the device is restored to working mode, paragraph [0083]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 1, Davis teaches the use of an image and configuration file pair.

In regards to claim 7, Gold discloses establishing a file transfer session between an information transferring network device that has entered a debug mode and a server includes:

- Establishing a first file transfer session with a first server, backup data being stored on the first server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050]).
- Determining whether the backup data is the last known good backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Establishing a second file transfer session with a second server, a second backup data being stored on the second server (Fig 1 shows a model of a sample network which contains M number of servers that can be used as backup servers).
- Determining whether the second backup data is the last known good backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Wherein the method further includes requesting a transfer of one of the first or second backup data that is the last known good backup data from the server to the network device (when a user selects to download, a data transfer module detects the correct version of the data to be loaded, and writes the data to the clients device, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 1, Davis teaches the use of an image and configuration file pair.

In regards to claim 8, Gold discloses a method comprising:

- Detecting that an information transferring network device has entered a debug mode, a name of a last known good backup data being stored on the network device (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).
- Establishing a first file transfer session between the network device and a first server, a first backup data being stored on the first server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050]).
- Determining whether the first backup data is the last known backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Establishing a second file transfer session between the network device and a second server, a second backup data being stored on the second server (Fig 1 shows a model of a sample network which contains M number of servers that can be used as backup servers).

- Determining whether the second backup data is the last known go backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Requesting a transfer of one of the first or second i backup data that is the last known good backup data from the server to the network device (when a user selects to download, a data transfer module detects the correct version of the data to be loaded, and writes the data to the clients device, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

Davis discloses a method of monitoring and recording critical system data in a device for initial program loading over a network. In the described invention, Davis teaches that a backup copy of a image and configuration file pair can be stored on a server to allow a client to load or boot a system with a reset initialization routine that will assure functionality (col 5 lines 15-42).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Gold's method of data backup and restoration to include utilizing an image and configuration file as taught by Davis to allow a client to load or boot a system with a reset initialization routine that will assure functionality.

In regards to claim 9, Gold discloses detecting the network device in fatal mode and entering the debug mode on the network device upon detecting the network device in fatal mode (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).

In regards to claim 10, Gold discloses receiving a command of a user and entering the debug mode on the network device upon receiving the command of the user (a user can choose to enter the debug mode to restore the backup data, paragraphs [0049] – [0053]).

In regards to claim 12, Gold discloses transfer of the last known backup data from the server to the network device (paragraph [0051]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 8, Davis teaches the use of an image and configuration file pair.

In regards to claim 13, Gold discloses automatically restoring the network device from debug mode to working mode after receiving the transfer of the last known backup data from the server to the network device (the transfer is starts, proceeds and finishes unattended which would show that the device is restored to working mode, paragraph [0083]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 8, Davis teaches the use of an image and configuration file pair.

In regards to claim 14, Gold discloses an apparatus comprising a machine accessible medium containing instructions which, when executed by a machine, cause the machine to perform operations comprising:

- Establishing a file transfer session between an information transferring network device that has entered a debug mode and a server, a name of a last known set of backup data being stored on the network device, the last known good backup data being stored on the server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050], the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Requesting a transfer of the last backup data from the server to the network device (the user requests the transfer of the backup files, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

Davis discloses a system of monitoring and recording critical system data in a device for initial program loading over a network. In the described invention, Davis teaches that a backup copy of a image and configuration file pair can be stored on a server to allow a client to load or boot a system with a reset initialization routine that will assure functionality (col 5 lines 15-42).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Gold's system of data backup and restoration to include utilizing an image and configuration file as taught by Davis to allow a client to load or boot a system with a reset initialization routine that will assure functionality.

In regards to claim 15, Gold discloses detecting the network device in fatal mode and entering the debug mode on the network device upon detecting the network device in fatal mode (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).

In regards to claim 16, Gold discloses receiving a command of a user and entering the debug mode on the network device upon receiving the command of the user (a user can choose to enter the debug mode to restore the backup data, paragraphs [0049] – [0053]).

In regards to claim 18, Gold discloses transfer of the last known backup data from the server to the network device (paragraph [0051]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 14, Davis teaches the use of an image and configuration file pair.

In regards to claim 19, Gold discloses automatically restoring the network device from debug mode to working mode after receiving the transfer of the last known backup data from the server to the network device (the transfer is starts, proceeds and finishes unattended which would show that the device is restored to working mode, paragraph

[0083]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 14, Davis teaches the use of an image and configuration file pair.

In regards to claim 20, Gold discloses establishing a file transfer session between an information transferring network device that has entered a debug mode and a server includes:

- Establishing a first file transfer session with a first server, backup data being stored on the first server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050]).
- Determining whether the backup data is the last known good backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Establishing a second file transfer session with a second server, a second backup data being stored on the second server (Fig 1 shows a model of a sample network which contains M number of servers that can be used as backup servers).
- Determining whether the second backup data is the last known good backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).

- Wherein the method further includes requesting a transfer of one of the first or second backup data that is the last known good backup data from the server to the network device (when a user selects to download, a data transfer module detects the correct version of the data to be loaded, and writes the data to the clients device, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 14, Davis teaches the use of an image and configuration file pair.

In regards to claim 21, Gold discloses an apparatus comprising a machine accessible medium containing instructions which, when executed by a machine, cause the machine to perform operations comprising:

- Detecting that an information transferring network device has entered a debug mode, a name of a last known good backup data being stored on the network device (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).
- Establishing a first file transfer session between the network device and a first server, a first backup data being stored on the first server (A user can establish a session with a backup server to restore data from the server to a networked device, paragraphs [0049] – [0050]).

- Determining whether the first backup data is the last known backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Establishing a second file transfer session between the network device and a second server, a second backup data being stored on the second server (Fig 1 shows a model of a sample network which contains M number of servers that can be used as backup servers).
- Determining whether the second backup data is the last known go backup data (the server containing a listing of the most recent backup files from the users computer, paragraphs [0043] – [0045]).
- Requesting a transfer of one of the first or second i backup data that is the last known good backup data from the server to the network device (when a user selects to download, a data transfer module detects the correct version of the data to be loaded, and writes the data to the clients device, paragraph [0051]).

Gold, however, lacks the specific backup files being an image and configuration file pair.

Davis discloses a method of monitoring and recording critical system data in a device for initial program loading over a network. In the described invention, Davis teaches that a backup copy of a image and configuration file pair can be stored on a server to allow a client to load or boot a system with a reset initialization routine that will assure functionality (col 5 lines 15-42).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Gold's method of data backup and restoration to include utilizing an

image and configuration file as taught by Davis to allow a client to load or boot a system with a reset initialization routine that will assure functionality.

In regards to claim 22, Gold discloses detecting the network device in fatal mode and entering the debug mode on the network device upon detecting the network device in fatal mode (in a disaster recovery mode, the networked device automatically enters debug mode and the backup data is loaded, paragraphs [0081] – [0083]).

In regards to claim 23, Gold discloses receiving a command of a user and entering the debug mode on the network device upon receiving the command of the user (a user can choose to enter the debug mode to restore the backup data, paragraphs [0049] – [0053]).

In regards to claim 25, Gold discloses transfer of the last known backup data from the server to the network device (paragraph [0051]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 21, Davis teaches the use of an image and configuration file pair.

In regards to claim 26, Gold discloses automatically restoring the network device from debug mode to working mode after receiving the transfer of the last known backup data from the server to the network device (the transfer is starts, proceeds and finishes

unattended which would show that the device is restored to working mode, paragraph [0083]). Gold, however, lacks the specific backup files being an image and configuration file pair.

As seen in the discussion of claim 21, Davis teaches the use of an image and configuration file pair.

Claims 4, 11, 17, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gold in view of Davis as applied to claims 1-3, 5-10, 11-16, 18-23, 25-26 above, and further in view of Sollins (The TFTP Protocol (Revision 2), RFC 1350, 1992, page 1).

Gold in view of Davis disclose a file transfer session, but lack utilizing the Trivial File Transfer Protocol (TFTP).

Sollins presents a memo on the features of the TFTP protocol. In this memo Sollins teaches that the TFTP protocol can be used to move files between machines on different networks easily as it has been implemented on top of the Internet User Datagram protocol, which allows for quick access utilizing a small simple, protocol.

It would have been obvious to one of ordinary skill in the art to modify Gold in view of Davis to utilize the TFTP protocol as taught by Sollins to allow easy access to files stored on a remote server as well as quick overall access utilizing a small, simple protocol.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Fletcher et al. (US Patent 6038379), a system for data backup and restore for a computer network utilizing a backup server and separate agents for various devices.
- Shaw (US Patent 6341373), a system for secure data downloading, recovery and upgrading utilizing a central backup server to serve several network devices.
- Whiteside et al. (EP 1227400 A2), a network based software recovery system utilizing a central backup server for multiple networked devices.
- Mickelsen (EP 1077411 A1), a system and method for restoring files on a computer network utilizing a data center for a client to backup files to for an emergency restoration of data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John R Brancolini whose telephone number is (703) 305-7107. The examiner can normally be reached on M-Th 7am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenton Burgess can be reached on (703) 305-4792. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JRB

ARID ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100